Série segurança, privacidade e anonimato – Introdução

By **Gabriel Camargo** 28/09/2022

Créditos da imagem: TI Fórum

Tempo estimado de leitura: 8 minutos

A série de artigos que hoje se inicia será um guia de segurança, privacidade e anonimato, focada, mas não exclusivamente contida, no mundo digital. Novas publicações serão lançadas todas as quartas-feiras, com profundidade progressiva de análise. Essa série faz parte de um projeto maior, o Guias Digitais, que poderá ser expandido para qualquer ramo relacionado à tecnologia.

A importância da segurança, privacidade e anonimato

Para iniciar nossa abordagem, devemos definir o nível de ameaça compatível. As estratégias utilizadas para a proteção digital de suas informações serão diferentes caso você queira se proteger de um possível ataque hacker, de uma infecção por malware ou do sistema de vigilância generalizada dos estados modernos.

Cada objetivo trará consigo uma diferente abordagem. Por isso, comece

definindo o que faz sentido para você. Ao longo dessa série de artigos, diversos métodos e ferramentas serão apresentados. Caberá ao leitor decidir o que fará sentido para o seu caso, dependendo do que e de quem se está querendo proteger.

Segurança, privacidade e anonimato estão interligados, porém, distintos. Segurança trata de restringir o acesso aos não autorizados, podendo ser o acesso aos seus arquivos, computadores ou servidores. Privacidade também está relacionada à restrição de acesso, contudo, privacidade se estende mesmo aos adversários confiáveis, do ponto de vista de segurança. Privacidade trata menos de esconder os participantes e mais de esconder o conteúdo e informações relacionadas.

Para uma abordagem estritamente privada, a identidade não assume importância central. Para o anonimato, sim. Em uma abordagem estritamente anônima, o foco não está na proteção do conteúdo e dados relacionados, mas nas identidades e relações entre os participantes, administradores ou possuidores de informações.

Sem privacidade, o desafio de obter segurança aumenta de forma considerável. Sua segurança também poderá depender de seu anonimato. Privacidade sem anonimato não será suficiente para a proteção de certas ameaças. No fim, os três se complementam, e sua complementação cruzada proporciona maior abrangência de proteção.

Um adendo importante

É comum a maioria das pessoas não se interessarem por esse assunto. Dos três, o mais interessante para o público geral é o primeiro: segurança. Com a gradual migração de serviços para o mundo digital, a capacidade de proteger contas de e-mail, redes sociais, dados bancários, dinheiro virtual, etc., torna a segurança um tópico atrativo aos que desejam maior proteção contra as ameaças da internet. Mesmo assim, o nível geral nesse quesito está muito abaixo do ideal.

Com relação à privacidade, sua importância geralmente não é entendida até o momento de sua perda. Um dos pensamentos mais comuns trata da questão dos anúncios online, com sua capacidade de rastreamento. Qual seria o problema de empresas me indicarem produtos relevantes? Por que deveria me esconder de empresas que estão querendo me prover serviços? Essas perguntas escondem a real natureza da questão.

Com a sempre crescente quantidade de dados sobre você, são

constantemente compartilhadas informações suas entre diferentes bancos de dados. Com isso, as Big Techs e agências governamentais de inteligência sabem desde todos os sites que você acessa até todos os seus interesses e opiniões. Um perfil cada vez mais completo e correto é então traçado, não apenas o que você quer comprar, mas também sobre como você pensa e enxerga o mundo.

O que as Big Techs sabem de você

Os dados coletados não são apenas utilizados para lhe vender produtos, algo que realmente não traria grandes problemas, mas os dados disponíveis também são utilizados para a classificação de indivíduos, para a sua colocação em listas de alvos potenciais, para a restrição de informações, etc. Esse problema será melhor abordado no segundo artigo dessa séria.

Dados disponíveis incluem informações detalhadas sobre você, sobre onde você está ou costuma ir, o que pesquisa, a religião que possui, sua preferência sexual, suas opiniões políticas, visitas a clínicas de aborto, prostíbulos ou sex shops, quais remédios foram por você comprados, quais igrejas foram por você visitadas, que religião você segue, seus dados pessoais, etc. Dados são a base das informações e informações, quando em posse de adversários, tornam-se armas.

O que hoje é feito sem maiores problemas, no futuro poderá ser encarado como tabu, algo errado mesmo criminoso. Reputações e imagens, ligadas a um histórico permanente de ações, também dificultam a empregabilidade futura. A perda total de privacidade e anonimato cria um mundo onde todos são constantemente vigiados, julgados e acusados, ficando todos vulneráveis as consequências de alguém mal-intencionado. A perda total de privacidade e anonimato também leva à perda parcial de segurança.

Um aviso importante

Aqui, uma observação. Esse guia não pretende auxiliar verdadeiros criminosos a esconder seus atos e evitar punições. O que aqui almejo é a proteção de indivíduos do rastreamento que consideram abusivo de empresas de tecnologia, bem como elevar o nível de proteção contra violência e ameaça, proveniente de diferentes fontes, desde outro usuário da internet até mesmo de agentes do estado. Ainda, ter algo a esconder não significa ter feito algo errado.

Todos nós temos informações que não compartilhamos com os outros, por motivos diversos, o que não significa que cometemos um erro ou mesmo

um crime. Criminosos tendem a querer se proteger, mas isso não implica ser criminoso aquele que deseja maior privacidade.

Mais sobre segurança, privacidade e anonimato

No artigo da próxima semana, serão apresentadas as capacidades dos diferentes adversários encontrados no mundo digital. Serão analisadas as capacidades de empresas de anúncio e rastreamento, big techs, hackers e agências governamentais de inteligência.

O terceiro artigo tratará de ações de nível básico, voltadas para uma maior porcentagem da população. Para aqueles que apenas desejam limitar o rastreamento de empresas como Meta e Google, bem como realizar mudanças simples, com baixo impacto de usabilidade e comodidade, mas com grande impacto na segurança, esse nível será suficiente.

O quarto artigo tratará do nível intermediário. Para aqueles que desejam praticamente eliminar o rastreamento realizado pelas Big Techs, aumentar ainda mais sua segurança e iniciar sua proteção pelo uso do anonimato, esse nível será suficiente. Aviso, contudo, que a adoção do proposto nesse nível demandará maior comprometimento que o anterior, bem como maiores limitações poderão desincentivar a adoção generalizada do que aqui será exposto.

O quinto artigo tratará do nível avançado. Para pessoas em situação vulnerável, como jornalistas, ativistas e pessoas em situação de vigilância direta, esse nível é o ideal. Alerto, contudo, que a **vigilância exercida por entidades poderosas, como NSA e CIA, não pode ser totalmente mitigada, mas pode ser dificultada ao ponto de não ser útil ao vigia, na relação de custo-benefício, ou dificultada ao ponto de garantir maior segurança ao usuário. Não há garantia de segurança total, no entanto, principalmente contra adversários poderosos e com orçamento ilimitado. Caso realmente queiram lhe encontrar e eliminar, provavelmente serão bem-sucedidos.**

Para os que quiserem se aprofundar ainda mais no assunto, links de referência e leitura adicional serão apresentados no sexto e último artigo.

Reforçando

Para finalizar esse artigo introdutório da série, retorno ao início. Cada um terá seu modelo de ameaça e diferentes modelos demandam diferentes

abordagens e profundidades. O que será feito aqui é apresentar possíveis problemas e possíveis soluções, que apenas se tornarão reais caso o seu modelo de ameaças as requirir.

Para o caso de usuários da internet que desejem restringir o rastreamento das big techs ou elevar sua segurança contra invasores, uma abordagem mais simples será suficiente para atingir esses resultados. Para a realização de uma contra economia, no entanto, níveis mais profundos de ameaças e soluções deverão ser analisados.

No fim, não existem soluções universais, por isso, cada leitor deverá entender aquilo que pretende proteger, aquilo que não se importa em compartilhar, de quem pretender proteger, o nível de usabilidade e comodidade que está disposto a renegar, bem como o nível de mudança de hábitos que está disposto a aceitar.

Não pense que não tenha nada a esconder, ou que você e seus dados não são interessantes o suficiente, o real valor da segurança, privacidade e anonimato apenas será entendido quando for tarde demais. **Por isso, iniciei essa série tratando do nível de ameaça. Ele definirá o que fará sentido para você e o que causa mais transtorno que benefício. Entendido isso, seguiremos com nosso guia.**

Tecnologia